



## Email Safety Tips

1. **Only open email attachments from contacts you know!** Be careful opening attachments from contacts you know, too. Friends may unwittingly send viruses or spyware if their computers are infected.
2. **Carefully read links before clicking them!** A common fraud technique is to slightly alter the web address of a website you go to regularly. A quick glance at the link and it would seem like you are going to a trusted website – but in reality you are being taken to a site that could attack your computer.
3. **Ensure your antivirus is up to date!** Viruses, Trojans, worms and spyware are constantly evolving and changing. Be sure to update your antivirus frequently to keep up with the changing environment!
4. **Always log out of your email account!** When using a library or public computer, sign yourself out of any websites to ensure nobody uses your account!
5. **Use a firewall.** “A firewall is a barrier that protects a computer or network from anyone who tries to access it from outside without authorization.” For more information on Firewalls, visit <http://www.scambusters.org/firewall.html>.
6. **Change your passwords frequently.** A good rule of thumb is to change your password every 30 – 90 days.
7. **Never share your passwords.** The best way to ensure that your email is secure is to be the only one using it!
8. **Do not reply to emails from unknown senders.** There are many scams that begin, “My dear friend.” These emails may come from a distant relative, a foreign “diplomat” or a stranger in need. These emails do not need to be responded to or even opened.
9. **Never share bank or personal information.**
10. **Use your noggin.** If something seems fishy or like a scam, it probably is. Trust your instincts.